



## **Administrative Policies and Procedures: 7.7**

---

### **Subject: Network Storage of Electronic Information**

Supersedes: DCS 7.7, 06/01/00

**Local Policy: No**

**Local Procedures: No**

**Training Required: No**

**Approved by:**

**Effective date: 06/01/00**

**Revision date: 02/01/03**

### **Application:**

To All Department of Children's Services and Community Service Agency Employees.

**Authority:** TCA 37-5-106, Management Advisory Committee

### **Policy:**

The purpose of this "Network Storage of Electronic Information Policy" is to establish guidelines and minimum requirements governing the storage location of electronic information. Establishing and maintaining compliance with this policy can lessen the risk to the Department of Children's Services of lost electronic information.

The objectives of this policy are to assure that:

- ◆ All electronic information created by users must be stored on the network drive (commonly referred to as the F: drive) and not the desktop computer drive (commonly referred to as the C: drive).
- ◆ Users understand that the storage of electronic information on the Desktop computer drive is highly susceptible to loss.
- ◆ Users understand that the storage of electronic information on the network drive is secure and is backed up on a nightly basis.
- ◆ Disruptions to state government activities from inappropriate storage of electronic information are avoided.

### **Procedures:**

#### **A. Storing electronic information**

1. All new computers installed after 02/01/2000 will have the default locations for saving electronic information set to the network (F:) drive.
2. The user will utilize this default setting for the storage of all electronic information that is vital to the business of the

Department of Children's Services and the State of Tennessee.

**B. Storage of electronic information outside network drive**

In the event that it is desirable to temporally store electronic information outside of the network drive location, the user must be aware that loss of electronic information is most likely not recoverable and accepts the risk.

**C. Internal Affairs & Internal Audit**

For added security, Internal Affairs and Internal Audit may utilize removable medium (diskettes, compact disks, audio tapes, video tapes, paper, etc.) for the storage of extremely sensitive documents. The removable medium should also have a backup in the event of unrecoverable damage.

**D. Storage Limits**

1. Storage of electronic information is limited. The limit in technical terms is 500 mega-bytes. This limit exceeds most business needs and is only in place as a precaution.
2. Storage of electronic information is limited to business related files only. Personal files such as music files are not authorized.
3. Periodic scans of the network will be performed to ensure compliance.

**Forms**

None

**Collateral Documents**

None

**Standards**

None

## **Glossary**

<b><i>Term</i></b>	<b><i>Definition</i></b>
<b><i>User (for this policy)</i></b>	A person that uses the computer.
<b><i>Medium</i></b>	Type of device used to store information, i.e., diskettes, compact disks, audiotapes, videotapes, paper.